



Wales Safer Communities Network response to: Home Office consultation on Ransomware Legislative Proposals

Closed 08 April 2025

Response submitted via electronic submission on the 08/04/2025

Q1. Are you responding to this survey as an individual or as a representative of an organisation?

Other:

The Wales Safer Communities Network: Responding on behalf of our members who deliver Community Safety across Wales, including- Policing in Wales, three Fire and Rescue Services, 22 Local Councils, Welsh Local Government Association, Probation and the Third Sector bodies

Q2. What is your age? *Please select one option*

Prefer not to say

Q3. What is your gender?

Prefer not to say

Q4. What is your ethnicity?

Prefer not to say

Q5. Which of the following options best describes the sector you work in? *If you are responding on behalf of an organisation, please select the sector of the organisation.*

Other:

The Network acts as a strategic voice for community safety in Wales, working collaboratively to champion and support community safety partnership working, and influence the shaping and development of national policy and local practice.

Responding on behalf of our members who deliver Community Safety across Wales, including- Policing in Wales, three Fire and Rescue Services, 22 Local Councils, Welsh Local Government Association, Probation and the Third Sector bodies.

Q7. How many people work for your organisation across the UK as a whole?

Prefer not to say

Q8. What is your organisation's annual turnover?

Prefer not to say



Q9. What part of the UK are you based in? If you are responding on behalf of an organisation, please select where your organisation is mainly based.

Wales

Proposal 1 - Targeted Ban on Ransomware Payments

Proposal 1: A ban on ransomware payments for all public sector bodies, including local government, and for owners and operators of Critical National Infrastructure (that are regulated, or that have competent authorities).

Scope Outline: The questions relating to this proposal are largely directed at those Critical National Infrastructure (CNI) owners and operators (who are regulated/have competent authorities) and the public sector, including local government, but we also welcome responses from others who have an interest in these sectors.

Please find the relevant information on Proposal 1: Targeted ban on ransomware payment in paragraphs 43-49 and Figure 2 of the accompanying consultation document.

Q10. To what extent do you agree, or disagree, that His Majesty's Government (HMG) should implement a targeted ban on ransomware payments for CNI owners and operators (who are regulated/have competent authorities) and the public sector, including local government?

Strongly Agree

Tend to agree

Neither agree nor disagree

Tend to disagree

Strongly disagree

Don't know

Q11. How effective do you think this proposed measure will be in reducing the amount of money flowing to ransomware criminals, and thus reducing their income?

Effective

Somewhat effective

Neither effective nor ineffective

Somewhat ineffective

Ineffective

Don't know



Q12. How effective do you think banning CNI owners and operators (who are regulated/have competent authorities) and the public sector, including local government, from making a payment will be in deterring cyber criminals from attacking them?

Effective

Somewhat effective

Neither effective nor ineffective

Somewhat ineffective

Ineffective

Don't know

Q13. What measures do you think would aid compliance with the proposed ban? Select all that apply.

Additional guidance to support compliance with the proposed ban

Tailored support to manage the response and impact following an attack

None

Don't know

Other (please specify):

Q14. What measures do you think are appropriate for non-compliance with the proposed ban? *Select all that apply.*

Criminal penalties for non-compliance

Civil penalties for non-compliance

None

Don't know

Other (please specify):

The Network feel that whilst most Public Services are already compliant with this proposal, by making it statute there is a clear message being sent which we support. In order to ensure this is seen as a legitimate security measure then appropriate investigation and financial penalties should be carried out should breaches be identified/ suspected.

Q15. If you represent a CNI organisation or public sector body, would your organisation need additional guidance to support compliance with a ban on ransomware payments?

Yes

No

Don't know

Not applicable



Q15a. As you responded yes to the previous question, what support would you need?

In response to any changes made there will need to be clear, visible and accessible guidance for all Public Services in English and in Welsh. With the purpose to understand what they should do if attacked, who and where to report incidents to, options available to them and a support system or number to call to discuss specific concerns. Whilst many may have these in place already, any guidance will need updating.

Q16. Should organisations within CNI and public sector supply chains be included in the proposed ban?

Yes

No

Don't know

Q16a. As you answered 'Yes' or 'No' to the previous question, please provide further explanation for your response (optional):

The Network feel that if an organisation is using public funds then there is a responsibility to look after the public interest. We therefore feel being included in this proposed ban is necessary

Q17. Do you think there should be any exceptions to the proposed ban?

Yes

No

Don't know

Q18. Do you think there is a case for widening the ban on ransomware payments further, or even imposing a complete ban economy-wide (all organisations and individuals)?

Yes widen the ban

Yes impose a complete ban economy-wide

No

Don't know

Proposal 2 - A New Ransomware Payment Prevention Regime

Proposal 2: A new ransomware payment prevention regime to cover all potential ransomware payments from the UK.



Scope Outline: The questions relating to this proposal are for all respondents.

Please find the relevant information on **Proposal 2: A new ransomware payment prevention regime** in paragraphs 50-62 and Figure 3 of the accompanying consultation document.

Q19. To what extent do you agree, or disagree, that the Home Office should implement the following:

	Strongly agree	Tend to agree	Neither agree nor disagree	Tend to disagree	Strongly disagree	Don't know
Economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1.	Strongly agree	Tend to agree	Neither agree nor disagree	Tend to disagree	Strongly disagree	Don't know
Threshold-based payment prevention regime, for certain organisations and individuals not covered by the ban set out in Proposal 1. <i>For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.</i>	Strongly agree	Tend to agree	Neither agree nor disagree	Tend to disagree	Strongly disagree	Don't know
Payment prevention regime for all organisations not covered by the ban set	Strongly agree	Tend to agree	Neither agree nor disagree	Tend to disagree	Strongly disagree	Don't know



<p>out in Proposal 1, but excluding individuals. <i>This would exclude individuals from the regime, but apply it to all organisations.</i></p>						
<p>Threshold-based payment prevention regime for certain organisations not covered by the ban set out in Proposal 1, excluding individuals. <i>This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.</i></p>	Strongly agree	Tend to agree	Neither agree nor disagree	Tend to disagree	Strongly disagree	Don't know

Please provide any further explanation for your response (optional):

We recognise, as identified in the consultation, that individuals and small business may feel they are not able to recover from reputational damage if the choice was taken away from them. Whilst in theory we would like to support a blanket ban, in practice this may be very damaging for individuals on a personal level and on the economy. However, we do wish to raise the concern that by not including all organisations and individuals there may be an inadvertent displacement towards them as a consequence of heightened measures.



Q20. How effective do you think the following will be in reducing ransomware payments?

	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know
Economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1.	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know
Threshold-based payment prevention regime, for certain organisations and individuals not covered by the ban set out in Proposal 1. <i>For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.</i>	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know
Payment prevention regime for all organisations not covered by the ban set out in Proposal 1, but excluding individuals. <i>This would exclude individuals from the regime, but apply it to all organisations.</i>	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know



Threshold-based payment prevention regime for certain organisations not covered by the ban set out in Proposal 1, excluding individuals. <i>This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.</i>	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know
--	------------------	--------------------	-----------------------------------	----------------------	-------------	------------

Q21. How effective do you think the following will be in increasing the ability of law enforcement agencies to intervene and investigate ransomware actors?

	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know
Economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1.	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know
Threshold-based payment prevention regime, for certain organisations and individuals not covered by the ban set out in Proposal 1.	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know



For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.						
Payment prevention regime for all organisations not covered by the ban set out in Proposal 1, but excluding individuals. <i>This would exclude individuals from the regime, but apply it to all organisations.</i>	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know
Threshold-based payment prevention regime for certain organisations not covered by the ban set out in Proposal 1, excluding individuals. <i>This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.</i>	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know

Q22. If we introduced a threshold-based payment prevention regime, what would be the best way to determine the threshold for inclusion? *Please select all that apply.*

Organisation's annual turnover in the UK
Organisation's number of employees in the UK
The sector the organisation is operating in
Amount of ransom demanded

Don't know

Other (please specify):

Q23. What measures do you think would aid compliance with a payment prevention regime? *Please select all that apply.*

Additional guidance to support compliance

Support to manage the response and impact following an attack



None

Don't know

Other (please specify):

Q24. Do you think these compliance measures need to be tailored to different organisations and individuals?

Yes

No

Q24a. As you responded 'Yes' to the previous question, please provide more details on how you think they should be tailored to different organisations and individuals and what, if any, alternative measures you would suggest? (optional)

As per a previous answer, it is important to understand that the needs of the support will need to compliment the asks of the ransom demand. Perhaps a phone line with advisors would be helpful to discuss needs directly would be helpful. However, having a toolkit, bank of information available for organisations/ individuals to access would be helpful.

Q25. What measures do you think are appropriate for managing non-compliance with a payment prevention regime? *Please select all that apply.*

Criminal penalties for non-compliance

Civil penalties for non-compliance

None

Don't know

Other (please specify):

Again, please see previous response. If measures are to be taken seriously there needs to be penalty implications, and we suggest fines would be helpful- as this would effectively counter the purpose of paying a ransom in the first place.

Q26. Do you think these non-compliance measures need to be tailored to different organisations and individuals?

Yes

No

Q27. For those reporting on behalf of an organisation, who do you think should be legally responsible for compliance with the regime?

The organisation

Named individual

Both



Don't know

Not applicable. I am responding as an individual

Q28. For those reporting on behalf of an organisation, do you think any measures for managing non-compliance with the regime should be the same for both the organisation and a named individual responsible for a ransomware payment?

Same

Different

Don't know

Not applicable. I am responding as an individual.

Please provide any additional comments (optional):

Whilst there should be internal procedures for named individuals responsible for any payments, in reality, organisations should be making these decisions as a collective and robust and appropriate policies and procedures need to be in place to safeguard any error or misunderstanding.

Proposal 3 - A Ransomware Incident Reporting Regime

Proposal 3: A ransomware incident reporting regime that could include a threshold-based mandatory reporting requirement for suspected victims of ransomware.

Scope Outline: The questions relating to this proposal are for all respondents.

Please find the relevant information on **Proposal 3: A ransomware incident reporting regime** in paragraphs 63-73 and Figure 4 of the accompanying consultation document.

Q29. To what extent do you agree, or disagree, that the Home Office should implement the following:

	Strongly agree	Tend to agree	Neither agree nor disagree	Tend to disagree	Strongly disagree	Don't know
Continuation of the existing voluntary ransomware incident reporting regime.	Strongly agree	Tend to agree	Neither agree nor disagree	Tend to disagree	Strongly disagree	Don't know



Economy-wide mandatory reporting for all organisations and individuals.	Strongly agree	Tend to agree	Neither agree nor disagree	Tend to disagree	Strongly disagree	Don't know
Threshold-based mandatory reporting, for certain organisations and individuals. <i>For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.</i>	Strongly agree	Tend to agree	Neither agree nor disagree	Tend to disagree	Strongly disagree	Don't know
Mandatory reporting for all organisations excluding individuals. <i>This would exclude individuals from the regime, but apply it to all organisations.</i>	Strongly agree	Tend to agree	Neither agree nor disagree	Tend to disagree	Strongly disagree	Don't know
Threshold-based mandatory reporting, for certain organisations excluding individuals. <i>This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.</i>	Strongly agree	Tend to agree	Neither agree nor disagree	Tend to disagree	Strongly disagree	Don't know

Q30. How effective do you think the following would be in increasing the Government's ability to understand the ransomware threat to the UK?

	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know
Continuation of the existing voluntary ransomware incident reporting regime	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know
Economy-wide mandatory reporting for all organisations and individuals.	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know



Threshold-based mandatory reporting, for certain organisations and individuals. <i>For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.</i>	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know
Mandatory reporting for all organisations excluding individuals. <i>This would exclude individuals from the regime, but apply it to all organisations.</i>	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know
Threshold-based mandatory reporting, for certain organisations excluding individuals. <i>This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.</i>	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know

Q31. How effective do you think the following would be in increasing the Government's ability to tackle and respond to the ransomware threat to the UK?

	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know
Continuation of the existing voluntary ransomware incident reporting regime.	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know
Economy-wide mandatory reporting for all organisations and individuals.	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know
Threshold-based mandatory reporting, for	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know



certain organisations and individuals. For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.						
Mandatory reporting for all organisations excluding individuals. <i>This would exclude individuals from the regime, but apply it to all organisations.</i>	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know
Threshold-based mandatory reporting, for certain organisations excluding individuals. <i>This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.</i>	Effective	Somewhat effective	Neither effective nor ineffective	Somewhat ineffective	Ineffective	Don't know

Q32. If we introduced a mandatory reporting regime for victims within a certain threshold, what would be the best way to determine the threshold for inclusion? *Please select all that apply.*

☐ Organisation's annual turnover in the UK
☐ Organisation's number of employees in the UK
☐ The sector organisation is operating in
☐ Amount of ransom demanded

Don't know

Other (please specify):

Q33. What measures do you think would aid compliance with a mandatory reporting regime? *Please select all that apply.*

Additional guidance to support compliance

Support to manage the response and impact following an attack

☐ None

☐ Don't know

Other (please specify):



Q34a. As you responded 'yes' to the previous question, please provide more details on how you think they should be tailored for different organisations and individuals and what, if any, alternative measures you would suggest? (optional)

As identified in the consultation, we are aware that current voluntary reporting is limited. Mandatory measures would help UK Govt and devolved administrations understand the larger picture and be able to tailor the response more effectively. However, as always, there will need to be clear guidance and structures in place that are available to organisations and individuals.

Q35. What measures do you think are appropriate for managing non-compliance with a mandatory reporting regime? *Please select all that apply.*

Criminal penalties for non-compliance

Civil penalties for non-compliance

None

Don't know

Other (please specify):

Q36. Do you think these non-compliance measures need to be tailored for different organisations and individuals?

Individual victims will need greater support, and likely be more vulnerable. Some may not know recognise that they are victims and others may not know how to report. A significant communication strategy would be needed to support this roll out as well as sufficient help and support

Q37. Do you think the presence of a mandatory incident reporting regime will impact business decisions of foreign companies and investors?

Yes

No

Don't know

Q38. For the mandatory reporting regime, is 72 hours a reasonable time frame for a suspected ransomware victim to make an initial report of an incident?

We think it would be better to say within one working week from the day of detection- this would allow ample time should there be planned leave or sickness absence. It would also provide 'breathing space' for individuals and organisations to come to terms with the situation they are in and seek advice



and guidance to act appropriately. 72 hours may not give enough time to do this

Q39. Do you think that an incident reporting regime should offer any of the following services to victims when reporting? *Please select all that apply.*

Support from cyber experts e.g. the National Cyber Security Centre (NCSC)/law enforcement

Guidance documents

Threat intelligence on ransomware criminals and trends

Operational updates e.g. activities law enforcement are undertaking.

Other (please specify):

Q40. Should mandatory reporting cover all cyber incidents (including phishing, hacking etc.), rather than just ransomware?

Yes

No

Don't know

Q41. Do you have any other comments on our consultation proposals?

Yes

No

Don't know